Read Book Technical Guide To Ipsec Virtual Private Networks Free Download Pdf

Virtual Private Networks Mar 17 2022 VPNs enable any enterprise to utilize the Internet as its own secure private network. In this book, two leading VPN implementers offer a start-to-finish, hands-on guide to constructing and operating secure VPNs. Going far beyond the theory found in most books, Ruixi Yuan and Tim Strayer present best practices for every aspect of VPN deployment, including tunneling, IPsec, authentication, public key infrastructure, and network/service management. Strayer and Yuan begin with a detailed overview of the fundamental concepts and architectures associated with enterprise VPNs, including site-to-site VPNs, remote access VPNs, and extranets. They compare all options for establishing VPN tunnels across the Internet, including PPTP, L2F, and L2TP. Next, they present in-depth coverage of implementing IPsec; establishing two-party or trusted third-party authentication; building a robust public key infrastructure; and managing access control. The book includes expert coverage of VPN gateway configuration, provisioning, and management; Windows and other VPN clients; and network/service management, including SLAs and network operations centers. Finally, the authors preview the future of VPNs, showing how they may be enhanced to provide greater quality of service and network intelligence. For all networking and IT professionals, security specialists, consultants, vendors, and service providers responsible for building or operating VPNs.

IPSec VPN Design Oct 24 2022 "IPSec VPN Design is the first book to present a detailed examination of the design aspects of IPSec protocols that enable secure VPN communication. - Divided into three parts, the book provides a solid understanding of design and architectural issues of large-scale, secure VPN solutions. Part I includes a comprehensive introduction to the general architecture of IPSec, including its protocols and Cisco IOS IPSec implementation details. - Part II examines IPSec VPN design principles covering hub-and-spoke, full-mesh, and fault-tolerant designs. This part of the book also covers dynamic configuration models used to simplify IPSec VPN designs. Part III addresses design issues in adding services to an IPSec VPN such as voice and multicast. - This part of the book also shows you how to effectively integrate IPSec VPNs with MPLS VPNs."--Jacket.

IPsec Virtual Private Network Fundamentals Nov 25 2022 This is the eBook version of the printed book. If the print book includes a CD-ROM, this content is not included within the eBook version. An introduction to designing and configuring Cisco IPsec VPNs Understand the basics of the IPsec protocol and learn implementation best practices Study up-to-date IPsec design, incorporating current Cisco innovations in the security and VPN marketplace Learn how to avoid common pitfalls related to IPsec deployment Reinforce theory with case studies, configuration examples showing how IPsec maps to real-world solutions IPsec Virtual Private N.

Comparing, Designing, and Deploying VPNs Jul 21 2022 A detailed guide for deploying PPTP, L2TPv2, L2TPv3, MPLS Layer-3, AToM, VPLS and IPSec virtual private networks.

IPSec Virtual Private Network Fundamentals Feb 28 2023 An introduction to designing and configuring Cisco IPsec VPNs Understand the basics of the IPsec protocol and learn implementation best practices Study up-to-date IPsec design, incorporating current Cisco innovations in the security and VPN marketplace Learn how to avoid common pitfalls related to IPsec deployment Reinforce theory with case studies, configuration examples showing how IPsec maps to real-world solutions IPsec Virtual Private Network Fundamentals provides a basic working knowledge of IPsec on various Cisco routing and switching platforms. It provides the foundation necessary to understand the different components of Cisco IPsec implementation and how it can be successfully implemented in a variety of network topologies and markets (service provider, enterprise, financial, government). This book views IPsec as an emerging requirement in most major vertical markets, explaining the need for increased information authentication, confidentiality, and non-repudiation for secure transmission of confidential data. The book is written using a layered approach, starting with basic explanations of why IPsec was developed and the types of organizations relying on IPsec to secure data transmissions. It then outlines the basic IPsec/ISAKMP fundamentals that were developed to meet demand for secure data transmission. The book covers the design and implementation of IPsec VPN architectures using an array of Cisco products, starting with basic concepts and proceeding to more advanced topics including high availability solutions and public key infrastructure (PKI). Sample topology diagrams and configuration examples are provided in each chapter to reinforce the fundamentals expressed in text and to assist readers in translating concepts into practical deployment scenarios. Additionally, comprehensive case studies are incorporated throughout to map topics to real-world solutions.

Implementing Virtual Private Networks Aug 10 2021 Annotation The first complete guide to the installation, operation, and management of Virtual Private Networks (VPN), a fast-growing technology framework that lets organizations use the Internet as their own private network. Shows how all the pieces of VPN architecture fit together: encryption, authentication, special network security considerations, and more. Takes readers step by step through VPN implementation, troubleshooting, maintenance, and ongoing security.

Pierre-Aristide Bréal Dec 22 2019

Virtual Private Networks Feb 16 2022 This book explains how to plan and build a Virtual Private Network (VPN), a collection of technologies that creates secure connections or "tunnels" over regular Internet lines. The book discusses costs, configuration, and how to install and use VPN technologies that are available for Windows NT and UNIX.

Virtual Private Networks For Dummies Sep 11 2021 Let’s face it: the information age makes dummies of us all at some point. One thing we can say for sure, though, about things related to the Internet is that their best strengths are often also their worst weaknesses. This goes for virtual private networks (VPNs). They may reach a wide base of customers – but can also be vulnerable to viruses, hackers, spoofers, and other shady online characters and entities. VPNs may allow for super-efficient communication between customer and company – but they rely on information which, if compromised, can cause huge losses. The Internet is still a frontier – sometimes so wide open it leaves us bewildered – and, like any frontier, the risks go hand in hand with potentially huge rewards. Virtual Private Networks for Dummies offers you a no-nonsense, practical guide to evaluating your company’s need for a VPN, understanding what it takes to implement one, and undertaking the challenging quest to set it up, make it work, and keep it safe. Whether you’re the resident expert leading the project team, or you just want to learn what makes e-commerce tick, this detailed, from-the-ground-up guide will soon have you comfortably conceptualizing: Security goals and strategies The evolution of VPNs Privacy in VPNs Extranets Remote-Access VPNs Funding Custom network solutions design Testing VPNs And more With new products and technologies offering supposedly revolutionary solutions to IT departments every day, this book focuses on the real world – you know, the one full of obstacles, mishaps, threats, delays, and errors – and gives you the background knowledge to make decisions for yourself about your VPN needs. Written with a dash of humor, Virtual Private Networks for Dummies contains both technical detail (standards, protocols, etc.) and more general concepts (such as conducting cost-benefit analyses). This clear, authoritative guide will have you securely and cost-effectively networking over the Internet in no time.

Juniper SRX Series May 07 2021 This complete field guide, authorized by Juniper Networks, is the perfect hands-on reference for deploying, configuring, and operating Juniper’s SRX Series networking device. Authors Brad Woodberg and Rob Cameron provide field-tested best practices for getting the most out of SRX deployments, based on their extensive field experience. While their earlier book, Junos Security, covered the SRX platform, this book focuses on the SRX Series devices themselves. You'll learn how to use SRX gateways to address an array of network requirements—including IP routing, intrusion detection, attack mitigation, unified threat management, and WAN acceleration. Along with case studies and troubleshooting tips, each chapter provides study questions and lots of useful illustrations. Explore SRX

components, platforms, and various deployment scenarios Learn best practices for configuring SRX's core networking features Leverage SRX system services to attain the best operational state Deploy SRX in transparent mode to act as a Layer 2 bridge Configure, troubleshoot, and deploy SRX in a highly available manner Design and configure an effective security policy in your network Implement and configure network address translation (NAT) types Provide security against deep threats with AppSecure, intrusion protection services, and unified threat management tools

Building and Integrating Virtual Private Networks with Openswan Mar 25 2020 Network administrators and any one who is interested in building secure VPNs using Openswan. It presumes basic knowledge of Linux, but no knowledge of VPNs is required.

Guide to IPsec VPNs Dec 02 2020 Internet Protocol Security (IPsec) is a widely used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over Internet Protocol (IP) networks. IPsec configuration is usually performed using the Internet Key Exchange (IKE) protocol. This publication provides practical guidance to organizations on implementing security services based on IPsec so that they can mitigate the risks associated with transmitting sensitive information across networks. The document focuses on how IPsec provides network layer security services and how organizations can implement IPsec and IKE to provide security under different circumstances. It also describes alternatives to IPsec and discusses under what circumstances each alternative may be appropriate.

Troubleshooting Virtual Private Networks May 27 2020 & Learn the troubleshooting techniques that every IT professional running a Virtual Private Network (VPN) must master & & Experience real-world solutions through practice scenarios in each chapter & & An essential workplace reference guide for every VPN management site

A Technical Guide to IPSec Virtual Private Networks May 19 2022 What is IPSec? What's a VPN? Why do the need each other? Virtual Private Network (VPN) has become one of the most recognized terms in our industry, yet there continuously seems to be different impressions of what VPNs really are and can become. A Technical Guide to IPSec Virtual Private Networks provides a single point of information that represents hundreds or resources and years of experience with IPSec VPN solutions. It cuts through the complexity surrounding IPSec and the idiosyncrasies of design, implementation, operations, and security. Starting with a primer on the IP protocol suite, the book travels layer by layer through the protocols and the technologies that make VPNs possible. It includes security theory, cryptography, RAS, authentication, IKE, IPSec, encapsulation, keys, and policies. After explaining the technologies and their interrelationships, the book provides sections on implementation and product evaluation. A Technical Guide to IPSec Virtual Private Networks arms information security, network, and system engineers and administrators with the knowledge and the methodologies to design and deploy VPNs in the real world for real companies.

IPSec Jan 27 2023 IPSec, Second Edition is the most authoritative, comprehensive, accessible, and up-to-date guide to IPSec technology. Two leading authorities cover all facets of IPSec architecture, implementation, and deployment; review important technical advances since IPSec was first standardized; and present new case studies demonstrating end-to-end IPSec security. New coverage also includes in-depth guidance on policies, updates on IPSec enhancements for large-scale enterprise environments, and much more.

Theoretical and Mathematical Foundations of Computer Science Aug 30 2020 This book constitutes the refereed post-proceedings of the Second International Conference on Theoretical and Mathematical Foundations of Computer Science, ICTMF 2011, held in Singapore in May 2011. The conference was held together with the Second International Conference on High Performance Networking, Computing, and Communication systems, ICHCC 2011, which proceedings are published in CCIS 163. The 84 revised selected papers presented were carefully reviewed and selected for inclusion in the book. The topics covered range from computational science, engineering and technology to digital signal processing, and computational biology to game theory, and other related topices.

Cisco Secure Virtual Private Networks Sep 23 2022 Based on the official instructor-led training course of the same name in a self-study product, Cisco® Secure Virtual Private Networks is a comprehensive, results-oriented book designed to give readers the knowledge to plan, administer, and maintain a Virtual Private Network (VPN). Readers are taught to accomplish several specific tasks, including identifying the features, functions, and benefits of Cisco® Secure VPN products; identifying the component technologies implemented in Cisco® Secure VPN products; utilizing commands required to configure and test IPSec in Cisco IOS® software and PIX Firewalls; installing and configuring the Cisco® VPN Client to create a secure tunnel to a Cisco® VPN Concentrator and PIX Firewall; configuring and verifying IPSec in the Cisco® VPN Concentrator, Cisco router, and PIX Firewall; and configuring the Cisco® VPN Concentrator, Cisco® router, and PIX Firewall for interoperability.

Guide to IPsec VPNs Jul 29 2020 Release date: December 2005 IPsec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection and access control. Why buy a book you can download for free? First you gotta find it and make sure it's the latest version, not always easy. Then you gotta print it using a network printer you share with 100 other people - and its outta paper - and the toner is low (take out the toner cartridge, shake it, then put it back). If it's just 10 pages, no problem, but if it's a 250-page book, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. An engineer that's paid $75 an hour has to do this himself (who has assistant's anymore?). If you are paid more than $10 an hour and use an ink jet printer, buying this book will save you money. It's much more cost-effective to just order the latest version from Amazon.com This public domain material is published by 4th Watch Books. We publish tightly-bound, full-size books at 8 1⁄2 by 11 inches, with glossy covers. 4th Watch Books is a Service Disabled Veteran Owned Small Business (SDVOSB) and is not affiliated with the National Institute of Standards and Technology. For more titles published by 4th Watch, please visit: cybah.webplus.net A full copy of all the pertinent cybersecurity standards is available on DVD-ROM in the CyberSecurity Standards Library disc which is available at Amazon.com. GSA P-100 Facilities Standards for the Public Buildings Service GSA P-120 Cost and Schedule Management Policy Requirements GSA P-140 Child Care Center Design Guide GSA Standard Level Features and Finishes for U.S. Courts Facilities GSA Courtroom Technology Manual NIST SP 500-299 NIST Cloud Computing Security Reference Architecture NIST SP 500-291 NIST Cloud Computing Standards Roadmap Version 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 1 & 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 3 DRAFT NIST SP 1800-8 Securing Wireless Infusion Pumps NISTIR 7497 Security Architecture Design Process for Health Information Exchanges (HIEs) NIST SP 800-66 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 800-177 Trustworthy Email NIST SP 800-184 Guide for Cybersecurity Event Recovery NIST SP 800-190 Application Container Security Guide NIST SP 800-193 Platform Firmware Resiliency Guidelines NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 1800-2 Identity and Access Management for Electric Utilities NIST SP 1800-5 IT Asset Management: Financial Services NIST SP 1800-6 Domain Name Systems-Based Electronic Mail Security NIST SP 1800-7 Situational Awareness for Electric Utilities DoD Medical Space Planning Criteria FARs Federal Acquisitions Regulation DFARS Defense Federal Acquisitions Regulations Supplement

IPSec Sep 30 2020 See:

VPNs Jan 15 2022 Beginners network professionals can learn how to set up a Virtual Private Network in the most secure and cost-effective way. Includes VPN blueprints for one of the fastest growing and secure methods for connecting branch offices.

Building VPNs Nov 01 2020 EASY-TO-FOLLOW EXAMPLES FOR SECURE, VERSATILE, COST-CUTTING, VALUE-ADDED VPNs With the security enhancements, flexibility, and market advantages now available with IPSec and MPLS, building mission-critical VPNs using these technologies has become a top agenda for many networking professionals. LEVERAGE THE BENEFITS OF IPSec AND MPLS Assembling a fully functional IPSec or MPLS VPN isn't easy. With so little information available it can be like trying to build a

bicycle when you have all the components, but no idea what the final product should look like. Only Building VPNs shows, in a clear, step-by-step fashion, how to build VPNs from scratch with IPSec and MPLS. Building VPNs: With IPSec and MPLS gives you: * From-the-ground-up directions for VPN construction * Step-by-step implementation of IPSec for secure, inexpensive, transmission of sensitive information across the public Internet * Easy-to-follow, diagrammed directions for deploying MPLS VPNs to provide value-added managed services * Clear instructions for using IPSec and MPLS in the enterprise and service-provider networking environments * Fully working solutions for both basic and advanced VPN issues * Examples that clarify every important step in VPN design, configuration, implementation, and deployment THE BOOK TO CHOOSE FOR VPN BUILDS

IKEv2 IPsec Virtual Private Networks Aug 22 2022

Building VPNs Feb 22 2020 Virtual Private Networks (VPNs) are a cheap and secure way for companies to transmit information over the Internet. With implementation of two new protocols, IPSec and MPLS, VPNs are about to become standard operating procedure. This guide aims to teach network engineers and architects, internetworking pros in the enterprise and service provider organisations and security pros working on VPNs as a corporate security measure how to use them. It walks readers through a VPN build from the ground up and demonstrates how IPSec and MPLS can be used in conjunction.

VPNs Illustrated Jun 08 2021

SSL Remote Access VPNs (Network Security) Feb 04 2021 SSL Remote Access VPNs An introduction to designing and configuring SSL virtual private networks Jazib Frahim, CCIE® No. 5459 Qiang Huang, CCIE No. 4937 Cisco® SSL VPN solutions (formerly known as Cisco WebVPN solutions) give you a flexible and secure way to extend networking resources to virtually any remote user with access to the Internet and a web browser. Remote access based on SSL VPN delivers secure access to network resources by establishing an encrypted tunnel across the Internet using a broadband (cable or DSL) or ISP dialup connection. SSL Remote Access VPNs provides you with a basic working knowledge of SSL virtual private networks on Cisco SSL VPN-capable devices. Design guidance is provided to assist you in implementing SSL VPN in existing network infrastructures. This includes examining existing hardware and software to determine whether they are SSL VPN capable, providing design recommendations, and guiding you on setting up the Cisco SSL VPN devices. Common deployment scenarios are covered to assist you in deploying an SSL VPN in your network. SSL Remote Access VPNs gives you everything you need to know to understand, design, install, configure, and troubleshoot all the components that make up an effective, secure SSL VPN solution. Jazib Frahim, CCIE® No. 5459, is currently working as a technical leader in the Worldwide Security Services Practice of the Cisco Advanced Services for Network Security. He is responsible for guiding customers in the design and implementation of their networks, with a focus on network security. He holds two CCIEs, one in routing and switching and the other in security. Qiang Huang, CCIE No. 4937, is a product manager in the Cisco Campus Switch System Technology Group, focusing on driving the security and intelligent services roadmap for market-leading modular Ethernet switching platforms. During his time at Cisco, Qiang has played an important role in a number of technology groups, including the Cisco TAC security and VPN team, where he was responsible for trouble-shooting complicated customer deployments in security and VPN solutions. Qiang has extensive knowledge of security and VPN technologies and experience in real-life customer deployments. Qiang holds CCIE certifications in routing and switching, security, and ISP Dial. Understand remote access VPN technologies, such as Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPsec), Layer 2 Forwarding (L2F), Layer 2 Tunneling (L2TP) over IPsec, and SSL VPN Learn about the building blocks of SSL VPN, including cryptographic algorithms and SSL and Transport Layer Security (TLS) Evaluate common design best practices for planning and designing an SSL VPN solution Gain insight into SSL VPN functionality on Cisco Adaptive Security Appliance (ASA) and Cisco IOS® routers Install and configure SSL VPNs on Cisco ASA and Cisco IOS routers Manage your SSL VPN deployment using Cisco Security Manager This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: SSL VPNs

VPNs Illustrated Jun 20 2022 Virtual private networks (VPNs) based on the Internet instead of the traditional leased lines offer organizations of all sizes the promise of a low-cost, secure electronic network. However, using the Internet to carry sensitive information can present serious privacy and security problems. By explaining how VPNs actually work, networking expert Jon Snader shows software engineers and network administrators how to use tunneling, authentication, and encryption to create safe, effective VPNs for any environment. Using an example-driven approach, VPNs Illustrated explores how tunnels and VPNs function by observing their behavior "on the wire." By learning to read and interpret various network traces, such as those produced by tcpdump, readers will be able to better understand and troubleshoot VPN and network behavior. Specific topics covered include: Block and stream symmetric ciphers, such as AES and RC4; and asymmetric ciphers, such as RSA and EIGamal Message authentication codes, including HMACs Tunneling technologies based on gtunnel SSL protocol for building network-to-network VPNs SSH protocols as drop-in replacements for telnet, ftp, and the BSD r-commands Lightweight VPNs, including VTun, CIPE, tinc, and OpenVPN IPsec, including its Authentication Header (AH) protocol, Encapsulating Security Payload (ESP), and IKE (the key management protocol) Packed with details, the text can be used as a handbook describing the functions of the protocols and the message formats that they use. Source code is available for download, and an appendix covers publicly available software that can be used to build tunnels and analyze traffic flow. VPNs Illustrated gives you the knowledge of tunneling and VPN technology you need to understand existing VPN implementations and successfully create your own.

Virtual Private Networks in Theory and Practice Oct 12 2021 Document from the year 2018 in the subject Computer Science - IT-Security, grade: A, language: English, abstract: This book encompasses virtual private network technologies theoretical as well as practical. In this project, it demonstrates how to VPNs actually work and their practical implementation with different lab scenarios step by step. The objective of this book is to teach the students and professionals in an easy way. The reader does not learn the theoretical knowledge of VPNs, but he also learns the practical implementation of several types of VPN in his home and office. There are several types of VPN with different scenarios. After the study of this book, the reader will be familiar with almost all types of VPN and can perform with different scenarios in his office and home.

IKEv2 IPsec Virtual Private Networks Mar 29 2023 Create and manage highly-secure Ipsec VPNs with IKEv2 and Cisco FlexVPN The IKEv2 protocol significantly improves VPN security, and Cisco’s FlexVPN offers a unified paradigm and command line interface for taking full advantage of it. Simple and modular, FlexVPN relies extensively on tunnel interfaces while maximizing compatibility with legacy VPNs. Now, two Cisco network security experts offer a complete, easy-tounderstand, and practical introduction to IKEv2, modern IPsec VPNs, and FlexVPN. The authors explain each key concept, and then guide you through all facets of FlexVPN planning, deployment, migration, configuration, administration, troubleshooting, and optimization. You’ll discover how IKEv2 improves on IKEv1, master key IKEv2 features, and learn how to apply them with Cisco FlexVPN. IKEv2 IPsec Virtual Private Networks offers practical design examples for many common scenarios, addressing IPv4 and IPv6, servers, clients, NAT, pre-shared keys, resiliency, overhead, and more. If you’re a network engineer, architect, security specialist, or VPN administrator, you’ll find all the knowledge you need to protect your organization with IKEv2 and FlexVPN. Understand IKEv2 improvements: anti-DDoS cookies, configuration payloads, acknowledged responses, and more Implement modern secure VPNs with Cisco IOS and IOS-XE Plan and deploy IKEv2 in diverse real-world environments Configure IKEv2 proposals, policies, profiles, keyrings, and authorization Use advanced IKEv2 features, including SGT transportation and IKEv2 fragmentation Understand FlexVPN, its tunnel interface types, and IOS AAA infrastructure Implement FlexVPN Server with EAP authentication, pre-shared keys, and digital signatures Deploy, configure, and customize FlexVPN clients Configure, manage, and troubleshoot the FlexVPN Load Balancer Improve FlexVPN resiliency with dynamic tunnel source, backup peers, and backup tunnels Monitor IPsec VPNs with AAA, SNMP, and Syslog Troubleshoot connectivity, tunnel creation, authentication, authorization, data encapsulation, data encryption, and overlay routing Calculate IPsec overhead and fragmentation Plan your IKEv2 migration: hardware, VPN technologies, routing, restrictions, capacity, PKI, authentication, availability, and more

The InfoSec Handbook Mar 05 2021 The InfoSec Handbook offers the reader an organized layout of information that is easily read and understood. Allowing beginners to enter the field and understand the

key concepts and ideas, while still keeping the experienced readers updated on topics and concepts. It is intended mainly for beginners to the field of information security, written in a way that makes it easy for them to understand the detailed content of the book. The book offers a practical and simple view of the security practices while still offering somewhat technical and detailed information relating to security. It helps the reader build a strong foundation of information, allowing them to move forward from the book with a larger knowledge base. Security is a constantly growing concern that everyone must deal with. Whether it's an average computer user or a highly skilled computer user, they are always confronted with different security risks. These risks range in danger and should always be dealt with accordingly. Unfortunately, not everyone is aware of the dangers or how to prevent them and this is where most of the issues arise in information technology (IT). When computer users do not take security into account many issues can arise from that like system compromises or loss of data and information. This is an obvious issue that is present with all computer users. This book is intended to educate the average and experienced user of what kinds of different security practices and standards exist. It will also cover how to manage security software and updates in order to be as protected as possible from all of the threats that they face.

A Technical Guide to IPSec Virtual Private Networks Apr 30 2023 What is IPSec? What's a VPN? Why do the need each other? Virtual Private Network (VPN) has become one of the most recognized terms in our industry, yet there continuously seems to be different impressions of what VPNs really are and can become. A Technical Guide to IPSec Virtual Private Networks provides a single point of information that represent

VPN - Virtual Private Networks Jan 03 2021 Studienarbeit aus dem Jahr 2003 im Fachbereich Informatik - Wirtschaftsinformatik, Note: 1,0, Universität Siegen, 12 Quellen im Literaturverzeichnis, Sprache: Deutsch, Abstract: Einleitung Virtual Private Networks, kurz VPNs, dienen dazu, zwei oder mehrere Rechner(netze) miteinander zu verbinden. Der Unterschied zu herkömmlichen, privaten Netzwerken ist dabei der Transportweg: VPNs nutzen öffentliche Netzwerke als Träger für den privaten Datenaustausch, so dass die Vernetzung von weit entfernten Rechnern(netzen) kein Problem darstellt. So gesehen handelt es sich bei Standfestverbindungen und Mietleitungen (z.B. mittels ISDN, Frame Relay und ATM), die bis heute bei der Verbindung von beispielsweise verteilten Unternehmensnetzen noch eine große Rolle spielen, definitionsgemäß auch um VPNs, da sie öffenliche Netze, wie das Telefonnetz, als Träger nutzen. Dennoch herrscht bei diesen Netzen die Vorstellung vor, es handele sich um private, physisch separate Netze. Das bekannteste und in Bezug auf VPN-Realisierungen zukunftsträchtigste öffentliche Netzwerk ist das Internet. Daher behandelt diese Arbeit ausschließlich die sogenannten Internet-VPNs, oder auch IP-VPNs. Die Größe des Internets und die Tatsache, dass praktisch Jedermann Zugriff darauf hat, macht eine Betrachtung der Sicherheit von VPNs nötig. Dabei wird diese Arbeit aufzeigen, dass diese Sicherheit von verschiedenen Faktoren abhängt, die sich durchaus beeinflussen lassen: Unter anderem muss eine Wahl der zu benutzenden Protokolle getroffen werden, wobei sich davon einige zum Standard etabliert haben, andere (noch) herstellereigene Lösungen sind. Weiterhin wird untersucht, inwieweit diese Protokolle in Betriebssystemen implementiert sind, d.h. man wird eine Vorstellung davon bekommen, wie geeignet Betriebssysteme sind, ein VPN aufzubauen. Als Alternative bieten sich Hardwarelösungen an, ein VPN einzurichten. Kapitel 5.3 beleuchtet einen Vertreter der Hardwarelösungen.

Virtual VPN in the Cloud Apr 06 2021 Cloud computing offers enterprises a method to access computing resources on-demand. This allows enterprises to save on capital expenses related to periodic hardware upgrades, maintenance and energy costs. However data traversing in cloud, leads to data breaching and data loss by third party intruders affecting the managing and reliability of sensitive information. A virtual private network, VPN, is a typical way of interconnecting networks over a public network infrastructure securing data transferred across the private subnets. The goal of this project is to provide VPN as a service using virtualized VPN software, essentially making the VPN yet another building block for a service in the cloud.

Set Up Your Own IPsec VPN, OpenVPN and WireGuard Server Nov 13 2021 Learn how to build your own VPN server in the cloud or on a Raspberry Pi This book is a comprehensive guide to building your own IPsec VPN, OpenVPN and WireGuard server. Based on 10 years of open source work with millions of users, this book covers everything you need to know to build your own VPN. Chapters 2 through 10 cover IPsec VPN installation, client setup and management, advanced usage, troubleshooting and more. Chapters 11 and 12 cover IPsec VPN on Docker and advanced usage. Chapters 13 through 15 cover OpenVPN installation, client setup and management. Chapters 16 through 18 cover WireGuard VPN installation, client setup and management. In the digital age, cyber security and privacy are more important than ever. Using a virtual private network (VPN) can help improve your cybersecurity and privacy by encrypting your network traffic, so that your data is protected as it travels via the Internet. This is especially useful when using unsecured Wi-Fi networks, such as at coffee shops, airports or in hotel rooms. Creating your own VPN server has become easier than ever, thanks to advances in technology such as affordable cloud servers and reduced bandwidth costs. Self-hosted VPNs can be considerably cheaper than commercial ones and offer several advantages. The VPN setup process can be fully automated and as simplified as possible. This book will help you build your own VPN server in the cloud or on a Raspberry Pi in just a few minutes. Get your copy of this book today and start building your own VPN!

Amazon Virtual Private Cloud Network Administrator Guide Apr 25 2020 Welcome to the Amazon VPC Network Administrator Guide. This guide is for customers who plan to use an AWS managed IPsec VPN connection with their virtual private cloud (VPC). The topics in this guide help you configure your customer gateway, which is the device on your side of the VPN connection. The VPN connection lets you bridge your VPC and IT infrastructure, and extend your existing security and management policies to EC2 instances in your VPC as if they were running within your own infrastructure.

Ip Sec. Vpn Design Apr 18 2022

IPSec VPN Design Dec 26 2022 The definitive design and deployment guide for secure virtual private networks Learn about IPSec protocols and Cisco IOS IPSec packet processing Understand the differences between IPSec tunnel mode and transport mode Evaluate the IPSec features that improve VPN scalability and fault tolerance, such as dead peer detection and control plane keepalives Overcome the challenges of working with NAT and PMTUD Explore IPSec remote-access features, including extended authentication, mode-configuration, and digital certificates Examine the pros and cons of various IPSec connection models such as native IPSec, GRE, and remote access Apply fault tolerance methods to IPSec VPN designs Employ mechanisms to alleviate the configuration complexity of a large- scale IPSec VPN, including Tunnel End-Point Discovery (TED) and Dynamic Multipoint VPNs (DMVPN) Add services to IPSec VPNs, including voice and multicast Understand how network-based VPNs operate and how to integrate IPSec VPNs with MPLS VPNs Among the many functions that networking technologies permit is the ability for organizations to easily and securely communicate with branch offices, mobile users, telecommuters, and business partners. Such connectivity is now vital to maintaining a competitive level of business productivity. Although several technologies exist that can enable interconnectivity among business sites, Internet-based virtual private networks (VPNs) have evolved as the most effective means to link corporate network resources to remote employees, offices, and mobile workers. VPNs provide productivity enhancements, efficient and convenient remote access to network resources, site-to-site connectivity, a high level of security, and tremendous cost savings. IPSec VPN Design is the first book to present a detailed examination of the design aspects of IPSec protocols that enable secure VPN communication. Divided into three parts, the book provides a solid understanding of design and architectural issues of large-scale, secure VPN solutions. Part I includes a comprehensive introduction to the general architecture of IPSec, including its protocols and Cisco IOS® IPSec implementation details. Part II examines IPSec VPN design principles covering hub-and-spoke, full-mesh, and fault-tolerant designs. This part of the book also covers dynamic configuration models used to simplify IPSec VPN designs. Part III addresses design issues in adding services to an IPSec VPN such as voice and multicast. This part of the book also shows you how to effectively integrate IPSec VPNs with MPLS VPNs. IPSec VPN Design provides you with the field-tested design and configuration advice to help you deploy an effective and secure VPN solution in any environment. This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks.

Building Linux Virtual Private Networks (VPNs) Dec 14 2021 The authors meet the growing demands of de-centralized companies that need a secure and functional network using Linux. The only book available that extensively covers the combination of VPN technology and Linux, this volume teaches first hand how to

build various VPN solutions with individual setup guides.
The Complete Cisco VPN Configuration Guide Jan 23 2020 With increased use of Internet connectivity and less reliance on private WAN networks, virtual private networks (VPNs) provide a much-needed secure method of transferring critical information. As Cisco Systems integrates security and access features into routers, firewalls, clients, and concentrators, its solutions become ever more accessible to companies with networks of all sizes. The Complete Cisco VPN Configuration Guide contains detailed explanations of all Cisco VPN products, describing how to set up IPsec and Secure Sockets Layer (SSL) connections on any type of Cisco device, including concentrators, clients, routers, or Cisco PIX and Cisco ASA security appliances. With copious configuration examples and troubleshooting scenarios, it offers clear information on VPN implementation designs. - A complete resource for understanding VPN components and VPN design issues - Learn how to employ state-of-the-art VPN connection types and implement complex VPN configurations on Cisco devices, including routers, Cisco PIX and Cisco ASA security appliances, concentrators, and remote access clients - Discover troubleshooting tips and techniques from real-world scenarios based on the author's vast field experience - Filled with relevant configurations you can use immediately in your own network
Guide to IPsec VPNs Jul 09 2021 IPsec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data & control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet. Contents of this Guide: Network Layer Security; IPsec Fundamentals; IPsec Planning & Implementation; Alternatives to IPsec; Planning & Implementation Case Studies; & Future Directions. Illustrations.
IPSec Base Virtual Private Network Jun 27 2020 "The Internet evolved from an experiential packet-switching network called the ARPANET. This network has grown exponentially since its conversion from an experimental to an operational network in 1975. However, the need for confidential and secure data channel has dissuaded many enterprises from using this ubiquitous public infrastructure. The IPSec protocol suite developed by the Internet Engineering Task Force (IETF) makes it possible to implement secure communication channels or virtual private network (VPN) over the Internet. Corporations can benefit from substantial financial savings by utilizing VPN for inter-company or intra-company communications rather than using expensive lease or privately own network infrastructure with its associated high maintenance costs. In this thesis, we will discuss the architecture, design and use of IPSec base VPN." --